INTERNET DOCUMENT INFORMATION FORM

A . Report Title: Securing, Protecting Critical U.S. Infrastructures

B. DATE Report Downloaded From the Internet: 24 Apr 98

C. Report's Point of Contact: (Name, Organization, Address, Office Symbol, & Ph # Robert T. Marsh, Chairman, President's Commission on Critical Infrastructure Protection

D. Currently Applicable Classification Level: Unclassified

E. Distribution Statement A: Approved for Public Release

F. The foregoing information was compiled and provided by: DTIC-OCA, Initials: __PM__ **Preparation Date**: 24 Apr 98

The foregoing information should exactly correspond to the Title, Report Number, and the Date on the accompanying report document. If there are mismatches, or other questions, contact the above OCA Representative for resolution.

DEFENSE ISSUES

The United States has worldwide military superiority, but it is approaching an age with threats that require new ways of thinking about America's vulnerabilities.

Volume 13, Number 3

Securing, Protecting Critical U.S. Infrastructures

Prepared remarks by Robert T. Marsh, chairman, President's Commission on Critical Infrastructure Protection, to the 20th National Information Systems Security Conference, Baltimore, Oct. 7, 1997.

Good morning, ladies and gentlemen. ... As you might imagine, it's a real busy time around the commission -- Our report is due to the president next week. ... I want to spend the next few minutes talking about the security and protection of our nation's critical infrastructures. ...

Imagine, if you will, that the power goes out in the Northwest. The 911 [service] is disrupted in a major city because someone has flooded the phone lines with repeat calls. Two bridges across the Mississippi River are destroyed -- bridges that not only carry trucks and trains, but also telephone cables; and two Internet service providers in New York City are out of service.

What do we do in such a situation? Who is in charge? Is it merely coincidence -- or a concentrated attack?

These are the types of questions the commission has been considering -- questions to which there are no easy answers; questions, we hope, our recommendations will help lay the foundation for answering.

This morning, I want to talk to you about the commission's work, our key findings, and then briefly summarize our recommendations. I must say right up front: Our findings, conclusions and recommendations are very different than we anticipated -- and different than our stakeholders anticipated.

Specifically, we discovered that protecting our infrastructures is a public-private undertaking and requires a new partnership, [and] protecting our infrastructures will take time and will require long-term efforts and a new way of thinking.

President Clinton established the commission last July and challenged us to recommend a national policy and implementation plan for protecting and assuring the nation's critical national infrastructures.

For the past year, we have been studying and analyzing the eight infrastructures -- or what I like to call the "life support systems." They are the backbone of our nation's defense and economic strength: telecommunications, electric power, transportation, oil and gas delivery and storage, water, emergency services and government services.

Critical infrastructures have long been lucrative targets for anyone wanting to attack another country. Once the Atlantic and Pacific oceans provided all the protection we needed.

That all changed during the Cold War. Technology became prevalent and geography became irrelevant. Soviet and U.S. nuclear weapons were targeted against each other's power grids, rail networks and energy industries. And in the Persian Gulf War, disabling Iraq's infrastructures was one of the keys to our success -- a lesson noted with interest by many countries around the world.

So why did the president bring together both private and public sector representatives to look at this

issue? Because waiting for a disaster to happen is a dangerous strategy. While a catastrophic cyber attack has not occurred, we have enough isolated incidents to know that the potential for disaster is real and the time to act is now!

The fact is our society depends on these infrastructures for its well-being and prosperity, the infrastructures are becoming increasingly dependent on one another [and], finally, both society and the infrastructures are increasingly susceptible to disruption by simple and easily accessible methods.

The commission and its oversight structure are uniquely tailored for this task. Recognizing that the critical infrastructures are largely owned and operated by the private sector, the commission structure represents public and private enterprise.

The commission is made up of representatives from both industry and government. The steering committee, which includes senior government officials, oversees the work of the commission and guides us through myriad government concerns. A presidentially appointed advisory committee of key industry leaders provides the unique perspective of owners and operators of the infrastructures.

The organization of the commission is significant, but what is also important is the thousands of people that we have met with as a part of our outreach effort. We held five regional public meetings, and participated in numerous conferences and simulations.

In total, we met with approximately 6,000 individuals from industry, academia, science, technology, the military and government. We sought to increase awareness of this issue through the media and through our web site. Just in case you haven't visited, we're located at http://www.pccip.gov.

Our outreach efforts were the initial steps to achieve one our most significant challenges: achieving private sector buy-in.

Since most of the infrastructures are privately owned and operated, we know that any solution that does not include private sector input and support is not a viable solution. Our goal is to lay the foundation for a public-private partnership that works together to protect our future.

Just why are we concerned about our infrastructures? What makes them so important? The answer is threefold: Our nation relies on its infrastructures for national security, public welfare and economic strength.

Those who choose to attack the infrastructures would do so to reduce our ability to act in our own interest, erode confidence in critical services or reduce American economic competitiveness.

Some significant changes in the world have further increased our concern about the infrastructures, and some of those forces have serious unintended side-effects. For example, global networks create somewhat of a double-edged sword. They enable us to communicate around the globe instantaneously, but they can create pathways for access to targeted systems -- thus introducing new vulnerabilities.

Deregulation and restructuring promote competition, lower cost, and improve efficiency. However, these same market forces can result in a diffusion of responsibility, a decrease in R&D [research and development] investment and reduced reserve.

While no one will argue that the U.S. has worldwide military superiority, adversaries are seeking new ways to fight us. They know they cannot win on the battlefield, so they seek "asymmetric" means, such as information warfare, to gain an advantage.

The bottom line is: We are approaching a new age with new threats, and it's going to require a new way of thinking about our vulnerabilities.

We have long understood the physical threats and vulnerabilities, but the rules change in cyberspace. The fast pace of technology means we are always catching up to understand the cyber dimension.

Furthermore, the "system of systems" we rely on for the daily operation of our critical infrastructures is increasingly interdependent and increasingly complex.

Finally, information that describes our vulnerabilities is increasingly accessible. Most of it is unclassified, and much of it is available on the Internet. We must be careful in compiling this information not to provide a handbook for those who would use it for harmful purposes.

So, who is the threat? We view the threat as anyone with the capability, technology and intent to do harm. While we have not found a "smoking keyboard," we do know that:

- The threat is a function of capability and intent;
- The capability to do harm is expansive and growing;
- The tools to do harm are readily available; and
- The opportunity to do harm is increasing.

The commission is focusing on getting ahead of this threat and we're doing that by trying to understand the tools of the perpetrators. There is a whole new arsenal of "weapons of mass disruption" in the cyber world -- "Trojan horses," viruses and e-mail attacks used to deny service or steal data. These tools recognize neither borders nor jurisdictions. They can be used anywhere, anytime, by anyone with the capability, technology and intent to do harm. I tend to call 'em "bad actors."

These bad actors range from the recreational hacker -- who thrives on the thrill and challenge of breaking into another's computer -- to the national security threat of information warriors intent on achieving strategic advantage.

Common to all threats is the insider. We could spend millions on technology to protect our infrastructures, but a well-placed insider or disgruntled employee could render nearly all protection useless. We also examined the respective roles of the private sector and the federal government in light of this new threat and the potential bad actors.

We concluded that the private sector has a responsibility to protect itself from the local threats, such as individual hackers and criminals. But the federal government has a larger responsibility to protect our citizens from national security threats. We found that national security is a shared responsibility.

In other words, the private sector is responsible for taking prudent measures to protect itself from commonplace hacker tools. If these tools are also used by the terrorist, then the private sector will also be protecting itself from cyberterrorist attack and will be playing a significant role in national security.

The federal government is responsible for collecting information about the tools, the perpetrators and their intent from all sources, including the owners and operators of the infrastructures. The government must share this information with the private sector so that industry can take the necessary protective measures.

Computers and electrons change the picture entirely. Now the capability is widely available at relatively little cost. This is the "new geography" in which the commission has focused its efforts. A few examples should illustrate the topography of technology in this new geography.

Langley Air Force Base [Va.] and several government and academic sites -- all of which prided themselves on their tight information security regimes -- were targets of a recent e-mail attack. A flood of e-mail messages originating in Australia and Estonia -- and routed through the White House computer system -- virtually shut down the air base's e-mail for hours until network administrators could filter out the "bad" messages.

Rome Laboratory in New York was the target in a computer intrusion. An individual in England used third-party countries (Latvia, Colombia and Chile) and commercial Internet service providers to gain access to Rome's computers, then launched attacks against a wide array of defense and government

computer systems.

The potential for damage ranges from accessing targeting information to causing loss of service to theft. We all have heard stories about loss of service to Internet service providers and theft of credit card data. Many other serious incidents are less well known, but include denial of 911 and emergency alerting systems.

Our findings indicate that:

- Both the capability for harm and the vulnerability of our infrastructures are serious risks.
- Neither the warning capability nor a nationwide analytic capability exist to protect our infrastructures from a concerted attack.
- Neither government nor industry are prepared to deal with these types of threats, nor do they share the relevant information that might give warning of a cyber attack.
- Finally, R&D efforts are not sufficient to address the cyber threat.

In short, the risk facing our infrastructures is shared among both the public and the private sectors. Thus we recommend first and foremost that government and industry work together to build a partnership for protection.

I'd like to take the opportunity now to briefly discuss some of our recommendations. All our recommendations were aimed at

improving coordination and establishing roles for infrastructure protection, fostering partnerships among all stakeholders and coordinating diverse interests.

The recommendations fall into several categories: steps the federal government should take, laying the foundation for a trusted environment necessary for improved information sharing, a nationwide education and awareness effort, conducting necessary research and development to build the tools for the future, supporting these recommendations through federal statutes, and building a partnership organization.

First, the federal government needs to lead by example before it can reach out to the private sector and other levels of government. We need to ensure the federal government has the policies and tools required to conduct business in the cyber age.

For example, we recommend the National Institute of Standards and Technology and the National Security Agency jointly set standards and publish best practices for information security -- and then share these with federal, state and local governments as well as with private industry. We also recommend federal agencies and departments be required to comply with these standards.

The commission also endorses a prototype system of encryption in collaboration with the private sector including implementing a key management infrastructure.

During our extensive outreach efforts, we heard time and again that the owners and operators of the infrastructures needed more information about cyber threats. They also said that a trusted environment must be built to allow the free exchange of information without fear of retribution, regulation or damage to reputation.

The first step to building the public-private partnership is creating a cooperative, collaborative information exchange within industry, within government, and between industry and government.

To facilitate this information flow, the commission recommends:

- Promoting private sector infrastructure information clearing centers;
- Providing anti-trust protection to encourage a free exchange;
- Protecting vulnerability information so that businesses can share information without fear of

compromising their competitive position; and
- Establishing a public-private information sharing, analysis, and warning center staffed by representatives from both industry and government.

The key to success of any of these initiatives is a concentrated effort to educate the American people about this new age and new threat. This is really a cultural change. We, therefore, recommend an education and awareness program that is aimed at all levels of education, from graduate programs to grammar school.

This includes grants by the National Science Foundation aimed at encouraging graduate-level research in network security and infrastructure protection; a series of conferences sponsored by the White House to spur new curricula in computer ethics and intellectual property for elementary and secondary schools; and partnership between the Department of Education and industry to develop curricula and market demand for educated and ethical technicians and managers.

We found that research and development efforts by the federal government are insufficient to deal with emerging cyber threats. Approximately $250 million is spent each year on infrastructure assurance, of which 60 percent, or $150 million, focuses on information security.

We identified very little R&D effort on the types of real-time detection, identification and response tools that the commission believes are necessary, and we also found that the market demand is currently insufficient to spur such development.

Consequently, we recommend a doubling of federal R&D funding for infrastructure protection to $500 million per year, with 20 percent increases each year for the next five years.

Implementing these recommendations will require updating relevant legal authorities and statues to accommodate the new cyber threat. Statutes such as the Defense Production Act, War Powers Resolution, Computer Security Act bear on our work, but all need to be updated to address cyber concerns.

Building the new partnership requires some principles of construction. We know this could not be another "big government" effort, but we know that government needs to set the example. We know that owners and operators are the key to success. We must build on existing organizations and relationships. We must rely on voluntary cooperation rather than mandates or regulation.

Finally, this is a long-term effort which requires continuous improvement. The commission has some specific proposals to facilitate identifying the information needed to best protect our infrastructure and sharing -- while protecting -- that information. These recommendations lay the foundation for establishing a "trusted environment" between the public-private sectors.

At the policy-making level, we will recommend creating the National Infrastructure Assurance Council -- a very high level advisory council comprised of senior CEOs [chief executive officers] from throughout the critical infrastructures, meeting regularly with selected Cabinet officers.

The council would propose policies and focus attention on infrastructure concerns. The purpose is to open the door of policy formulation to include the private sector owners and operators -- those who are closest to the problem and best know the range of solutions.

We will also recommend establishing a focal point for infrastructure protection within the White House to coordinate the federal government's efforts, including research and development. These two offices will be supported by an Infrastructure Assurance Support Office within the Department of Commerce.

At the operational level, our recommendations focus on enhancing industry and government's information exchange, including:

- Organizing sector infrastructure assurance "clearinghouses," most likely building on an existing

association or industry group, that best suit each infrastructure's information sharing needs. In essence, each industry will select an entity to coordinate that industry's various participants and to identify, collect, desensitize and disseminate necessary information related to infrastructure protection.
- Designating federal agencies to facilitate establishing these clearinghouses and to provide any necessary government support.
- Finally, and perhaps our most novel recommendation, creating a public-private information warning and analysis center staffed by both government and industry representatives.

Their job will be to receive relevant information from the sector clearinghouses and various government agencies, analyze this information to assess what is happening in the infrastructures, decide on the necessary measures to be taken, determine best practices, and disseminate needed information to both government and industry.

The sum of these efforts is to create flexible, reliable channels for information to flow between industry and government.

Just as the risks are shared between the public and the private sectors, so will the solutions will be found. Our national and economic security has become a shared responsibility, one that will require a new kind of partnership between government and industry, one which encourages information sharing and one which will require the government to lead by example.

We have the opportunity to get ahead of a problem before it becomes a crisis. The commission is laying the foundation, and we challenge people like you and organizations like yours to continue to build upon our research.

Published for internal information use by the American Forces Information Service, a field activity of the Office of the Assistant Secretary of Defense (Public Affairs), Washington, D.C. Parenthetical entries are speaker/author notes; bracketed entries are editorial notes. This material is in the public domain and may be reprinted without permission.

DEFENSE ISSUES

INDEX